

# Set Families with Low Pairwise Intersection

Calvin Beideman  
High School  
mathematicsfan@gmail.com

Jeremiah Blocki  
Carnegie Mellon University  
jblocki@cs.cmu.edu

April 18, 2014

## Abstract

A  $(n, \ell, \gamma)$ -sharing set family of size  $m$  is a family of sets  $S_1, \dots, S_m \subseteq [n]$  s.t. each set has size  $\ell$  and each pair of sets shares at most  $\gamma$  elements. We let  $m(n, \ell, \gamma)$  denote the maximum size of any such set family and we consider the following question: How large can  $m(n, \ell, \gamma)$  be?  $(n, \ell, \gamma)$ -sharing set families have a rich set of applications including the construction of pseudorandom number generators [NW94] and usable and secure password management schemes [BBD13]. We analyze the explicit construction of Blocki et al [BBD13] using recent bounds [Son09] on the value of the  $t$ 'th Ramanujan prime [Ram19]. We show that this explicit construction produces a  $(4\ell^2 \ln 4\ell, \ell, \gamma)$ -sharing set family of size  $(2\ell \ln 2\ell)^{\gamma+1}$  for any  $\ell \geq \gamma$ . We also show that the construction of Blocki et al [BBD13] can be used to obtain a *weak*  $(n, \ell, \gamma)$ -sharing set family of size  $m$  for *any*  $m > 0$ . These results are competitive with the inexplicit construction of Raz et al [RRV99] for weak  $(n, \ell, \gamma)$ -sharing families. We show that our explicit construction of weak  $(n, \ell, \gamma)$ -sharing set families can be used to obtain a parallelizable pseudorandom number generator with a low memory footprint by using the pseudorandom number generator of Nisan and Wigderson [NW94]. We also prove that  $m(n, n/c_1, c_2 n)$  must be a constant whenever  $c_2 \leq \frac{2}{c_1^3 + c_1^2}$ . We show that this bound is nearly tight as  $m(n, n/c_1, c_2 n)$  grows exponentially fast whenever  $c_2 > c_1^{-2}$ .

## 1 Introduction

Informally, we define an  $(n, \ell, \gamma)$ -sharing set family of size  $m$  to be a collection of  $m$  subsets of  $[n]$ , each of size  $\ell$ , no two of which have more than  $\gamma$  elements in common, and we let  $m(n, \ell, \gamma)$  denote the maximum size of such a set family. How large can  $m(n, \ell, \gamma)$  be? Can we find explicit constructions of large  $(n, \ell, \gamma)$ -sharing set families? While these combinatorial questions are interesting in their own right, these question also have numerous practical implications including the construction of pseudorandom number generators [NW94], randomness extractors [Tre01, RRV99] and most recently usable and secure password management scheme (systematic strategies for users to create and remember multiple passwords) [BBD13].

**Applications to Pseudorandom Number Generation** A pseudorandom number generator is a function  $\mathbf{G} : \{0, 1\}^n \rightarrow \{0, 1\}^m$  which takes a uniformly random seed  $x \sim \{0, 1\}^n$  of length  $n$ , and outputs a string  $\mathbf{G}(x) \in \{0, 1\}^m$  ( $m \gg n$ ) which “looks random.” Nisan and

Wigderson used a  $(n, \ell = O(\sqrt{n}), \gamma = \log m)$ -sharing set family  $\mathcal{S} = \{S_1, \dots, S_m\}$  of size  $m$  to construct pseudorandom number generators [NW94]. In particular, they define the pseudorandom number generator  $\mathbf{NW}_{P,\mathcal{S}}(x) = P(x_{|S_1}) \dots P(x_{|S_m})$ , where  $x_{|S_i} \in \{0, 1\}^\ell$  denotes the bits of  $x \in \{0, 1\}^\ell$  at the indices specified by  $S_i$  and  $P : \{0, 1\}^\ell \rightarrow \{0, 1\}$  is a predicate. If the predicate  $P : \{0, 1\}^\ell \rightarrow \{0, 1\}$  is “hard” for circuits of size  $H_\ell(P)$  to predict<sup>1</sup> then no circuit of size  $H_\ell(P) - O(m2^\gamma)$  will be able to distinguish  $\mathbf{NW}_{P,\mathcal{S}}(x)$  from a truly random binary string of length  $m$ , when the seed  $x \sim \{0, 1\}^n$  is chosen uniformly at random. In this context,  $n$  is the length of the random seed,  $m$  is the number of random bits extracted and the pseudorandom number generator fools circuits of size  $H_\ell(P) - O(m2^\gamma)$ . Thus, we would like to find  $(n, \ell, \gamma)$ -sharing set families where  $n$  is small,  $m$  is large (e.g., we can extract many pseudorandom bits from a small seed) and  $\gamma$  is small (e.g., so that the pseudorandom bits look random to a large circuit). Nisan and Wigderson gave an explicit construction of an  $(\ell^2, \ell, \gamma)$ -sharing set family of size  $\ell^{\gamma+1}$ .

**Applications to Randomness Extractors** Trevisan used the pseudorandom number generator of Nisan and Wigderson to construct a randomness extractor [Tre01]. A  $(k, \epsilon)$  randomness extractor is a function  $\mathbf{Ext} : \{0, 1\}^{\hat{\ell}} \times \{0, 1\}^n \rightarrow \{0, 1\}^m$  that takes a string  $x_1 \sim D$ , where  $D$  is a distribution over  $\{0, 1\}^{\hat{\ell}}$  with minimum entropy  $k$ , along with a  $n$  additional uniformly random bits  $x_2 \sim \{0, 1\}^n$  and extracts an  $m$ -bit string  $y \in \{0, 1\}^m$  that is almost uniformly random (e.g., distribution over  $y \in \{0, 1\}^m$  is  $\epsilon$ -close to the uniform distribution  $U_m$  over  $\{0, 1\}^m$ ). Trevisan used the string  $x_1$  to select a random predicate  $P : \{0, 1\}^{\hat{\ell}} \rightarrow \{0, 1\}$ , and then extracted  $m$  bits by running  $\mathbf{NW}_{P,\mathcal{S}}(x_2)$ . Raz et al [RRV99] observed that the pseudorandom number generator Nisan and Wigderson could be built using a *weak*  $(n, \ell, \gamma)$ -sharing set family of size  $m$ , and showed how to construct *weak*  $(n, \ell, \gamma)$ -sharing set family of size  $m$  for *any* value of  $m$  as long as  $n \geq \lceil \frac{\ell}{\gamma} \rceil \ell$ . However, their construction was not explicit.

**Advantages of Explicit Constructions** One nice property of the Nisan Wigderson Pseudorandom number generator is that it is highly parallelizable. For each  $j \in [m]$  we can compute the  $j$ 'th bit  $\mathbf{NW}_{P,\mathcal{S}}(x)[j] = P(x_{|S_j})$  independently as long as we can quickly find the set  $S_j \in \mathcal{S}$ . Observe that we would need space at least  $O(m\ell \log n)$  to store the set family  $\mathcal{S} = \{S_1, \dots, S_m\}$ , which could be a problem especially when  $m$  is very large. However, if the set family has an explicit construction (e.g., there is a small circuit  $C$  s.t.  $C(i) = S_i$  for all  $i \in [m]$ ) then we can simply compute  $\mathbf{NW}_{P,\mathcal{S}}(x)[j] = P(x_{|C(j)})$ .

**Applications to Password Management** Recently Blocki et al [BBD13] used  $(n, \ell, \gamma)$ -sharing set families to develop usable and secure password management schemes. In their proposed password management scheme, Shared Cues, the user memorizes and rehearses  $n$  secret stories. From these  $n$  stories the user is able to create  $m(n, \ell, \gamma)$  different passwords. In particular, the password at each of the user's accounts is formed by appending  $\ell$  of these secret stories together. A usable password management scheme should keep  $n$  and  $\ell$  as small as possible so that the user does not have to memorize too many stories and type too many

---

<sup>1</sup>Nisan and Wigderson observe that a random predicate  $P$  will satisfy this property with high probability [NW94].

stories when he logs into an account.  $\gamma$  is a security parameter which specifies how much information one password might leak about another (e.g., if an adversary learns the user’s Amazon password then he learns at most  $\gamma$  of the user’s stories for eBay). A secure password management scheme should keep  $\gamma$  as small as possible (so that one password does not leak too much information about another password) and  $\ell$  as large as possible (so that each password has high entropy). Blocki et al [BBD13] gave a construction of  $(n, \ell, \gamma)$ -sharing set families using the Chinese Remainder Theorem. Given pairwise coprime numbers  $n_1, \dots, n_\ell$  s.t.  $n = n_1 + \dots + n_\ell$  they construct  $S_1, \dots, S_m$  where  $S_i = \{1 + \sum_{k=1}^{j-1} n_k + (i \bmod n_j) : j \in [\ell]\}$ . They use the Chinese Remainder Theorem to prove that  $\max_{i \neq j} |S_i \cap S_j| \leq \gamma$  as long as  $m \leq \prod_{i=1}^{\gamma+1} n_i$ .

**Contributions** We analyze the explicit construction of Blocki et al [BBD13] and show that it is competitive with the explicit construction of Nisan and Wigderson [NW94]. Our analysis uses recent bounds [Son09] on the value of the  $t$ ’th Ramanujan prime [Ram19]. We also show that the construction of Blocki et al can be used to explicitly construct *weak*  $(n, \ell, \gamma)$ -sharing set families whose size is very large. Our analysis shows that this explicit construction is competitive with the non-explicit construction of Raz et al [RRV99]. We show that our explicit construction of weak  $(n, \ell, \gamma)$ -sharing set families can be used to obtain a parallelizable pseudorandom number generator with a low memory footprint by using the pseudorandom number generator of Nisan and Wigderson [NW94]. We also prove several upper bounds on the value of  $m(n, \ell, \gamma)$  when  $\ell$  and  $\gamma$  are in a constant ratio to  $n$ .

**Organization** The paper is organized as follows: We first introduce related work in Section 1.1. We then introduce preliminary definitions in Section 2. In Section 3 we analyze the construction of Blocki et. al, and state a lower bound on  $m(n, \ell, \gamma)$  that can be derived from it. We compare this lower bound to the construction of Nisan and Wigderson. We also show that this explicit construction yields a good *weak*  $(n, \ell, \gamma)$ -sharing set family. In Section 4 we explain how the explicit construction of Blocki et al [BBD13] can be used to obtain a highly parallelizable pseudorandom number generator with a low memory footprint. In Section 5 we explore some cases where  $\ell$  and  $\gamma$  are in a constant ratio to  $n$  and prove an upper bound on  $m(n, \ell, \gamma)$  as  $n$  grows large. We show that our upper bounds are nearly tight. We conclude in Section 6 by discussing cases that do not meet the conditions for any of our bounds, and hypotheses about how our bounds could be made stronger.

## 1.1 Related Work

The problem of finding maximally sized  $(n, \ell, \gamma)$ -sharing set families was considered at least as early as 1956 by Paul Erdős and Alfréd Rényi [ER56], and applications of some of these families may have been considered by Euler [Eul82]. Erdős explored properties of these families several times [EH63] [EFF85], and Rödl built on his work [Röd85].

$(n, \ell, \gamma)$ -sharing set families were rediscovered by Nisan and Wigderson [NW94], who used them to design a pseudorandom number generator. Trevisan showed how to use  $(n, \ell, \gamma)$ -sharing set families to construct pseudorandom extractors [Tre01]. Extractors are algorithms that transform weakly random sources into a uniformly random source. Raz et al [RRV99] improved on Trevisan’s pseudorandom extractors by introducing a weakened

notion of  $(n, \ell, \gamma)$ -sharing set families. They require that the set family  $S_1, \dots, S_m \subseteq [n]$  satisfies  $|S_i| = \ell$  and  $\sum_{j < i} 2^{|S_i \cap S_j|} \leq 2^\gamma (m - 1)$  for all  $i \in [m]$  (instead of  $|S_i \cap S_j| \leq \gamma$ ). Observe that every  $(n, \ell, \gamma)$ -sharing set family also satisfies these weaker requirements. Using this relaxed definition Raz et al [RRV99] showed how to extract a uniformly random string  $y \in \{0, 1\}^k$  using at most  $O(\log^3 n)$  bits of information given a string  $x \in \{0, 1\}^n$  chosen at random from a distribution  $D$  with minimum entropy  $k$ . To obtain their results they show how to construct very large *weak*  $(n, \ell, \gamma)$ -sharing set families. However, their construction is not explicit. We use the construction of Blocki et al to obtain an explicit construction of large *weak*  $(n, \ell, \gamma)$ -sharing set families.

Blocki et al [BBD13] proposed a construction of  $m$   $(n, \ell, \gamma)$ -sharing set families based on the Chinese Remainder Theorem. In their analysis of their construction they focused on parameters that were appropriate for the context of password management (e.g.,  $\ell = 4, \gamma = 1, n = 43$ ). We extend their analysis to include a broader range of parameters. Our analysis uses recent results of Sondow [Son09], who provided a (nearly) asymptotically tight bound on the value of the  $t$ 'th Ramanujan prime [Ram19]. We show that the construction of Blocki et al [BBD13] yields a larger  $(n, \ell, \gamma)$ -sharing set family than the construction of Nisan and Wigderson [NW94] with equivalent values of  $n$  and  $\gamma$  (though the value of  $\ell$  is slightly smaller).

## 2 Preliminaries

We begin by formally defining an  $(n, \ell, \gamma)$ -sharing set family (Definition 1).

**Definition 1.** *An  $(n, \ell, \gamma)$ -sharing set family  $S_1, \dots, S_m \subseteq [n]$  of size  $m$  satisfies the following conditions: (1)  $\forall i \in [m]. |S_i| = \ell$ , and (2)  $\forall 1 \leq i < j \leq m. |S_i \cap S_j| \leq \gamma$ . We use  $m(n, \ell, \gamma)$  to denote the maximum value of  $m$  such that there exists an  $n, \ell, \gamma$  sharing set family of size  $m$ . We say that a set family  $S_1, \dots, S_m \subseteq [n]$  is explicitly constructible if there is a circuit  $C$  of size  $O(n)$  that computes  $C(i) = S_i$  for each  $i \in [m]$ .*

Nisan and Wigderson referred to these families as  $(k, m)$ -designs [NW94]. We follow the notation of Blocki et al [BBD13]. The construction of Blocki et al [BBD13] relies on the Chinese Remainder Theorem. To analyze their construction we will be interested in finding a large set  $S = \{t_1, \dots, t_\ell\}$  of integers such that  $S$  has size  $\ell$ , the numbers in  $S$  are pairwise coprime,  $\sum_{i=1}^\ell t_i \leq n$  and each  $t_i \geq \frac{n}{2\ell}$ . We will rely on recent results on prime density.

**Definition 2.**  $\pi(t)$  indicates the number of prime numbers less than or equal to  $t$ .  $\pi\pi(t)$  indicates the maximum  $|S|$  such that  $S \subseteq \{\lceil \frac{t}{2} \rceil, \dots, t\}$  and  $\forall i \neq j \in S. \text{GCD}(i, j) = 1$ .

We are particularly interested in lower bounding the value  $\pi\pi(x)$ . Clearly,  $\pi\pi(x) \geq \pi(x) - \pi(x/2)$ . As it turns out this lower bound is nearly tight (see Theorem 4). We can bound  $\pi(x) - \pi(x/2)$  using Ramanujan primes.

**Definition 3.** [Ram19] *The  $t$ 'th Ramanujan Prime is the smallest integer  $R_t$  s.t.  $\pi(x) - \pi(x/2) \geq t$  for all  $x \geq R_t$ .*

Allowing  $n$  to equal at least  $\ell R_\ell$  guarantees that  $\{\frac{n}{2\ell}, \frac{n}{\ell}\}$  contains at least  $\ell$  primes which will satisfy the conditions of the Blocki conjecture. Sondow's bounds on Ramanujan primes (see Theorem 2) allow us to express this bound on  $n$  as an elementary function.

## 2.1 Pseudorandom Number Generators and Randomness Extractors

Before we formally define a pseudorandom number generator we first define a pseudorandom distribution  $X$  over  $\{0, 1\}^m$ . Informally, definition 4 say that distribution is pseudorandom a distribution that ‘appears’ random to any ‘small enough’ circuit. Given a circuit  $C$  we use

$$\mathbf{Adv}_C(X) = \left| \Pr_{x \in X}[C(x) = 1] - \Pr_{x \in U_m}[C(x) = 1] \right|$$

to denote the advantage of  $C$  at predicting whether  $x$  was drawn from the distribution  $X$  or from  $U_m$ , where  $U_m$  is the uniform distribution over  $\{0, 1\}^m$ . The distribution  $X$  ‘appears’ random to a circuit  $C$  if  $\mathbf{Adv}_C(X)$  is small.

**Definition 4.** A distribution  $X$  over  $\{0, 1\}^m$  is said to be  $(s, \epsilon)$ -pseudorandom if, given any circuit  $C$  (taking  $m$  inputs) of size at most  $s$ ,  $\mathbf{Adv}_C(X) \leq \epsilon$ .

Given a distribution  $X$  over  $\{0, 1\}^n$  and a function  $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$  we use  $G(X)$  to denote the distribution over  $\{0, 1\}^m$  induced by  $G$ . Informally, a function  $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$  is pseudorandom if it induces a pseudorandom distribution.

**Definition 5.** Let  $\{G_n\}_{n \in \mathbb{N}}$  be a family of functions such that  $G_n : \{0, 1\}^n \rightarrow \{0, 1\}^m$ . We say the family is a  $(s, \epsilon)$ -pseudorandom number generator if  $G$  is computable in time  $2^{O(n)}$ , and  $G(U_n)$  considered as a distribution is  $(s, \epsilon)$ -pseudorandom.

Nisan and Wigderson [NW94] show how to construct a pseudorandom number generator  $G : \{0, 1\}^n \rightarrow \{0, 1\}^m$  using any  $(n, \ell, \gamma)$ -sharing set family of size  $m$ . Their construction assumes the existence of a predicate  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$  that is hard for ‘small’ circuits to predict.

**Definition 6.** Let  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$  be a boolean function. We say that  $f$  is  $(s, \epsilon)$ -hard if for any circuit  $C$  of size  $s$ ,  $\left| \Pr_{x \sim \{0, 1\}^\ell}[C(x) = f(x)] - \frac{1}{2} \right| \leq \epsilon$ .

Observe that a random function will fool all small circuits with high probability<sup>2</sup>. Following, Nisan and Wigderson we use  $H(f)$  to denote the hardness of a function  $f$ .

**Definition 7.** Let  $f : \{0, 1\}^* \rightarrow \{0, 1\}$  be a boolean function and let  $f_\ell$  be the restriction of  $f$  to strings of length  $\ell$ . The hardness of  $f$  at  $\ell$ ,  $H_f(\ell)$  is defined to be the maximum integer  $h_\ell$  such that  $f_\ell$  is  $(1/h_\ell, h_\ell)$ -hard.

Raz et al [RRV99] showed that the Nisan-Wigderson pseudorandom number generator works even if the family of sets  $S_1, \dots, S_m$  only satisfies the weaker condition from definition 8. Observe that any  $(n, \ell, \gamma)$ -sharing set family is also a *weak*  $(n, \ell, \gamma)$ -sharing set family, but the converse is not necessarily true. We also note that as  $m$  increases the requirement  $\sum_{j < i} 2^{|S_i \cap S_j|} \leq 2^\gamma(m-1)$  becomes increasingly lax. This allows us to construct arbitrarily large weak  $(n, \ell, \gamma)$ -sharing families.

**Definition 8.** A family of sets  $S_1, \dots, S_m \subset [n]$  is a *weak*  $(n, \ell, \gamma)$ -sharing set family if (1)  $\forall i \in [m]. |S_i| = \ell$ , and (2)  $\forall i \in [m]. \sum_{j < i} 2^{|S_i \cap S_j|} \leq 2^\gamma(m-1)$ .

<sup>2</sup>The argument is straightforward. Fix any circuit  $C$ . A random function  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$  will satisfy  $\mathbf{Adv}_C(f(U_\ell)) \leq \epsilon$  with very high probability by Chernoff bounds. We can then apply union bounds to argue that a random  $f$  will satisfy  $\max_{C \in \mathcal{C}} \mathbf{Adv}_C(X) \leq \epsilon$  for any sufficiently small class  $\mathcal{C}$  of circuits.

### 3 Constructions

Nisan and Wigderson [NW94] gave an explicit construction of  $(\ell^2, \ell, \gamma)$ -sharing set families of size  $m = \ell^{\gamma+1}$  for any prime power  $\ell$ . Given a polynomial  $p(x)$  with coefficients in  $\mathbf{GF}(\ell)$ , the finite field of size  $\ell$ , they define the set  $S_p = \{(x, p(x)) \mid x \in \mathbf{GF}(\ell)\}$ . The family  $\mathcal{S} = \{S_p \mid p \text{ has degree } \leq \gamma\}$  is  $(\ell^2, \ell, \gamma)$ -sharing and has size  $m = |\mathcal{S}| = \ell^{\gamma+1}$ . Given pairwise coprime numbers  $n_1 < \dots < n_\ell$  Blocki et al [BBD13] provided an explicit construction of  $(\sum_{i=1}^\ell n_i, \ell, \gamma)$ -sharing families. Given an integer  $i \geq 0$  they define the set  $S_i = \{1 + \sum_{k=1}^{j-1} n_k + (i \bmod n_j) : j \in [\ell]\}$ . They show that the family  $\mathcal{S} = \{S_i \mid 0 \leq i < \prod_{j=1}^{\gamma+1} n_j\}$  is an  $(\sum_{i=1}^\ell n_i, \ell, \gamma)$ -sharing set family of size  $\prod_{j=1}^{\gamma+1} n_j$ .

The proof of Theorem 3 is based on the following result of Blocki et al [BBD13]. We take advantage of Sondow's results on prime density [Son09] to compare the Blocki et al construction to the construction of Nisan and Wigderson.

**Theorem 1.** [BBD13] *Suppose that  $n_1 < \dots < n_\ell$  are pairwise co-prime then there is a  $(\sum_{i=1}^\ell n_i, \ell, \gamma)$ -sharing set system of size  $m = \prod_{i=1}^\ell n_i$ . Furthermore, this set family has an explicit construction.*

**Theorem 2.** [Son09] *For all  $t \geq 1$  the following bound holds  $2t \ln t < R_t < 4t \ln 4t$ .*

**Theorem 3.**  $\forall n \geq 4\ell^2 \ln 4\ell$ ,  $m(n, \ell, \gamma) \geq (2\ell \ln 2\ell)^{\gamma+1}$ . *Furthermore, this set family is explicitly constructible.*

*Proof.* Theorem 2 due to Sondow [Son09] shows that there will always be at least  $\ell$  primes  $p_1, \dots, p_\ell$  between  $2\ell \ln 2\ell$  and  $4\ell \ln 4\ell$ . We have  $\sum_{i=1}^\ell p_i \leq \ell(4\ell \ln 4\ell) \leq n$ . Note that  $\prod_{i=1}^{\gamma+1} p_i \geq (2\ell \ln 2\ell)^{\gamma+1}$ . It follows from Theorem 1 that  $m(n, \ell, \gamma) \geq (2\ell \ln 2\ell)^{\gamma+1}$ .  $\square$

Note that the construction of Blocki et al only requires relatively prime numbers. So the results from theorem 3 could be improved by including non-prime values. However, theorem 4 implies that these improvements will not be particularly significant.

**Theorem 4.**  $\forall n \in \mathbb{Z}^+$ .  $\pi\pi(n) \leq \pi(n) - \pi(\frac{n}{2}) + \pi(\sqrt{n})$ .

*Proof.* Let  $S \subseteq \{\lceil \frac{n}{2} \rceil, \dots, n\}$  be a set of coprime numbers of maximum size. Observe that each prime number  $p \in [n]$  is a factor of at most one number in  $S$ . Without loss of generality we can assume that each of the primes between  $n$  and  $\frac{n}{2}$  are contained in  $S$  (if  $p \notin S$  then, because  $S$  is of maximum size, we must have some  $t = pq \in S$ , but in this case we can simply replace  $t$  with  $p$ ). The number of primes between  $n$  and  $\frac{n}{2}$  is  $\pi(n) - \pi(\frac{n}{2})$ , and all of these integers are relatively prime to each other and to every other number in the range  $[n]$ . All other numbers in  $S$  must have at least two prime factors, and at least one of them must be less than or equal to  $\sqrt{n}$ . Since each prime factor less than or equal to  $\sqrt{n}$  can be used at most once, for the members of  $S$  to remain pairwise relatively prime, at most  $\pi(\sqrt{n})$  non-primes can be included in the set, each containing a single prime factor less than  $\sqrt{n}$ .  $\square$



**Comparison.** To compare the constructions of Blocki et al [BBD13] and Nisan and Wigderson [NW94] we set  $n = 4\ell'^2 \ln 4\ell'$  and we set  $\ell = \sqrt{4\ell'^2 \ln 4\ell'}$ . The construction of Nisan and Wigderson gives use  $m(n, \ell, \gamma) \geq \ell^{\gamma+1} = \left(2\ell' \sqrt{\ln 4\ell'}\right)^{\gamma+1}$ , while the construction of Blocki et al [BBD13] gives us  $m(n, \ell', \gamma) \geq (2\ell' \ln 2\ell')^{\gamma+1} > \left(2\ell' \sqrt{\ln 4\ell'}\right)^{\gamma+1}$ . However,  $\ell' < \ell$  so the construction of Blocki et al has a smaller  $\ell$ .

### 3.1 Constructing Weak $(n, \ell, \gamma)$ -sharing set families

In this subsection we show that the techniques of Blocki et al [BBD13] yield an explicit construction of weak  $(n, \ell, \gamma)$ -sharing set families of arbitrary size  $m$ . Our main results are stated in Theorem 5.

**Theorem 5.** *For all  $m$  there is an explicitly constructible weak  $(4\ell^2 \ln 4\ell, \ell, \gamma)$ -sharing set family of size  $m$  as long as  $2^\gamma \geq \left(1 + \frac{1}{-1 + \ln 2\ell}\right)$ . Furthermore, this set family is explicitly constructible.*

*Proof.* Let  $m$  be given. We use the explicit construction of Blocki et al [BBD13]. By Theorem 2 we can find  $\ell$  primes such that  $2\ell \ln 2\ell < p_1 < \dots < p_\ell < 4\ell \ln 4\ell$ . In particular, we let  $S_i = \left\{1 + \sum_{k=1}^{j-1} p_k + (i \bmod p_j) \mid j \in [\ell]\right\}$ . Now for  $i \in [m]$  we have

$$\begin{aligned} \sum_{j < i} 2^{|S_i \cap S_j|} &= \sum_{k=0}^{\infty} 2^k |\{j \mid j < i \wedge |S_i \cap S_j| = k\}| \leq \sum_{k=0}^{\infty} 2^k |\{j \mid j < i \wedge |S_i \cap S_j| \geq k\}| \\ &\leq \sum_{k=0}^{\infty} 2^k \binom{\ell}{k} \frac{i-1}{\prod_{j=1}^k p_j} \leq \sum_{k=0}^{\infty} 2^k \binom{\ell}{k} \frac{i-1}{(2\ell \ln 2\ell)^k} \\ &\leq \sum_{k=0}^{\infty} \frac{i-1}{(\ln 2\ell)^k} \leq (i-1) \left( \frac{\ln 2\ell}{-1 + \ln 2\ell} \right) \leq (m-1) 2^\gamma \end{aligned}$$

□

Raz et al gave a randomized construction of weak  $\left(\left\lceil \frac{\ell}{\gamma} \right\rceil \cdot \ell, \ell, \gamma\right)$ -sharing set families for any  $m, \gamma > 0$ . While they showed that their construction could be derandomized, their construction is not explicit (e.g., the construction of  $i$ 'th subset  $S_i$  is dependent on the sets  $S_1, \dots, S_{i-1}$ ). Our analysis shows that the construction of Blocki et al [BBD13] is competitive with the construction of Raz et al [RRV99] though the value of  $n$  is slightly larger.

## 4 Parallel Pseudorandom Number Generators

Nisan and Wigderson proved that if  $\gamma = \log m$ ,  $\mathcal{S}$  is a  $(n, \ell, \gamma)$ -sharing set family and  $H_f(\ell) \geq 2m^2$  that their construction  $\mathbf{NW}_{f, \mathcal{S}}$  is a  $(m^2, \frac{1}{m})$  pseudorandom number generator. In particular, Theorem 6 implies that if  $D$  is a circuit of size  $|D| \leq m^2$  that distinguishes  $\mathbf{NW}_{f, \mathcal{S}}(U_n)$  from  $U_m$  with advantage  $\mathbf{ADV}_D(\mathbf{NW}_{f, \mathcal{S}}(U_n)) \geq \frac{1}{m}$  then there exists a circuit

$C$  of size  $|C| \leq 2m^2$  which predicts  $f(x)$  with advantage  $\mathbf{ADV}_C(f(U_\ell)) \geq \frac{1}{2m^2}$ . This contradicts the definition of  $H_f(\ell)$ . Raz et al [RRV99] observed that it suffices for  $\mathcal{S}$  to be a weak  $(n, \ell, \gamma)$ -sharing set family. If we let  $\mathcal{S}_m$  denote the explicitly constructible weak  $(4\ell^2 \ln 4\ell, \ell, \gamma)$ -sharing set family of size  $m$  from Section 3.1 then for any  $m > 0$   $\mathbf{NW}_{f, \mathcal{S}_m}$  is a  $(m^2, \frac{1}{m})$  pseudorandom number generator with seed length  $4\ell^2 \ln 4\ell$  assuming that  $H_f(\ell) \geq 2m^2$ . Because  $\mathcal{S}_m$  is explicitly constructible we can compute each bit  $\mathbf{NW}_{f, \mathcal{S}_m}(x)[i] = f(x_{|S_i})$  independently.

**Theorem 6.** [NW94, RRV99] Let  $f : \{0, 1\}^\ell \rightarrow \{0, 1\}$  be a boolean function and  $\mathcal{S} = \{S_1, \dots, S_m\}$  be an weak  $(n, \ell, \gamma)$ -sharing set family. Suppose  $D : \{0, 1\}^m \rightarrow \{0, 1\}$  is such that  $\mathbf{ADV}_D(\mathbf{NW}_{f, \mathcal{S}}(U_n)) > \epsilon$ , then there exists a circuit  $C$  of size  $|C| \leq |D| + O\left(\max_{j \in [m]} \sum_{i < j} 2^{|S_i \cap S_j|} m\right)$  such that  $\left|\Pr_{x \sim \{0, 1\}^\ell} [C(x) = f(x)] - \frac{1}{2}\right| \geq \frac{\epsilon}{m}$

## 5 Upper Bounds

Our main result in this section is Theorem 7. We prove that  $m(n, \ell, \gamma) = c_1$  whenever  $\ell = \frac{n}{c_1}$  and  $\gamma = c_2 n$  provided that  $c_2$  is sufficiently small. Blocki et al proved that  $m(n, \ell, \gamma) \leq \frac{\binom{n}{\ell}}{\binom{\gamma+1}{\ell}}$ . We note that this bound is far from tight whenever  $\ell$  is large. For example, if  $c_1 = 2$  and  $c_2 = \frac{1}{10}$  then the upper bound of Blocki et al  $\frac{\binom{n}{\ell}}{\binom{\gamma+1}{\ell}} = \frac{\binom{n}{\frac{n}{2}}}{\binom{\frac{n}{2}+1}{\frac{n}{2}}}$  grows exponentially with  $n$ . By contrast, Theorem 7 implies that  $m(n, n/2, n/10) = 2$ .

**Theorem 7.**  $\forall 0 < c_2 < 1, n, c_1 \in \mathbb{N}$  such that  $c_1 | n$ .  $m(n, \frac{n}{c_1}, c_2 n) = c_1$  iff  $c_2 < \frac{2}{c_1^3 + c_1^2}$ .

The proof of Theorem 7 can be bound in the appendix. We instead prove an easier result here. Theorem 8 upper bounds  $\lim_{n \rightarrow \infty} m(n, \ell, \gamma)$  when  $\ell$  is in a constant ratio to  $n$  and  $\gamma$  is small. Theorem 8 holds because the  $k$ 'th set  $S_k$  must use  $cn - (k-1)\gamma$  new elements (elements that are not in  $\bigcup_{i=1}^{k-1} S_i$ ).

**Theorem 8.**  $\forall \gamma_c, 0 < c < 1$  such that  $cn \in \mathbb{N}$ .  $m(n, cn, \gamma_c) \rightarrow \lfloor \frac{1}{c} \rfloor$  as  $n \rightarrow \infty$ .

*Proof.* Let  $\ell = cn$  and let  $\tau \in \mathbb{N}$  be an integer such that  $\tau > \lfloor \frac{1}{c} \rfloor$ . The first set will contain  $\ell$  elements. The second set can share at most  $\gamma$  of them, so the second set must contain at least  $\ell - \gamma$  previously unused elements. Therefore the union of the first two sets must contain at least  $2\ell - \gamma$  elements. In a similar manner, the  $k$ th set must contain at least  $\ell - (k-1)\gamma$  new elements, therefore,

$$k\ell - \frac{(k-1)k\gamma}{2} \leq \left| \bigcup_{i=1}^k S_i \right| \leq n. \quad (1)$$

Assume for contradiction that  $\limsup_{n \rightarrow \infty} m(n, cn, \gamma_c) = \tau$ . Then we have

$$\begin{aligned} \lim_{n \rightarrow \infty} \left( n - \tau\ell + \frac{(k-1)k\gamma}{2} \right) &= \lim_{n \rightarrow \infty} \left( n - \tau cn + \frac{(k-1)k\gamma}{2} \right) \\ &= \lim_{n \rightarrow \infty} (n(1 - c\tau)) \\ &= -\infty. \end{aligned}$$

This contradicts equation 1. □



We also show that the upper bound from Theorem 7 is nearly tight. In particular, when  $\gamma = c_2 n$  for a slightly larger constant  $c_2$  then  $m(n, \ell, \gamma)$  is exponentially large. Theorem 9 lower bounds the values of  $c_2$  for which  $m(n, \ell, \gamma)$  is exponentially large.

The full proof of Theorem 9 is found in the appendix. We demonstrate the existence of an  $(n, \ell, \gamma)$ -sharing set family of exponential size by showing that the probability of obtaining such a set family through random selection is non-zero. Our proof uses the following randomized construction of an  $(n, \ell, \gamma)$ -sharing set family. Independently choose random integers  $r_i^j$  each in the range  $0 \leq r_i < c_1$  for  $i \in \{0, \dots, \ell - 1\}$  and  $j \in [m]$ . Let  $S_j = \bigcup_{i=0}^{\ell-1} \{ic_1 + r_i^j\}$ . We use standard concentration bounds due to Chernoff [Che52] to show that  $|S_j \cap S_j| \leq \gamma$  with high probability, and then we union bounds to argue that the entire set family is  $(n, \ell, \gamma)$ -sharing with non-zero probability.

**Theorem 9.**  $\forall c_2 > 0, n, c_1 \in \mathbb{N}$  such that  $c_1 |n$ .  $m(n, \frac{n}{c_1}, c_2 n) > \exp(O(n))$  if  $c_2 > \frac{1}{c_1^2} + \epsilon$ .

Blocki et al [BBD13] observed that  $m(n, \gamma + 1, \gamma) = \binom{n}{\gamma+1}$  whenever  $n \geq \gamma + 1$ . We observe that in general  $m(n, \ell, \gamma) \geq m(n, \ell + 1, \gamma)$  whenever  $\ell \geq \gamma + 1$ <sup>3</sup>. This implies that whenever  $n/2 \geq \gamma + 1$  we have

$$\max_{\ell \geq \gamma} m(n, \ell, \gamma) = m(n, \gamma + 1, \gamma) = \binom{n}{\gamma + 1},$$

and whenever  $\gamma \geq n/2$  we have  $\max_{\ell \geq \gamma} m(n, \ell, \gamma) = m(n, \gamma, \gamma) = \binom{n}{\gamma}$ . Clearly, the inequality  $m(n, \ell, \gamma) \geq m(n, \ell, \gamma + 1)$  also holds. Both of these inequalities also hold for weak  $(n, \ell, \gamma)$ -sharing set families.

## 6 Open Questions

We conclude with some open questions.

We have shown that the explicit construction of Blocki et al [BBD13] can be used with the weaker requirements of Raz et al [RRV99] to create weak  $(n, \ell, \gamma)$ -sharing set families of arbitrarily large size. Our analysis uses a number of potentially loose bounds, however, so it is possible that a better analysis of the Blocki et al construction for weak set families could improve our requirements on the parameters. Also of interest is whether there is another explicit construction that would perform better than the Blocki et al construction.

We have shown that the value  $m(n, n/c_1, nc_2)$  is constant whenever  $c_2 \leq \frac{2}{c_1^3 + c_1^2}$ . Furthermore, we showed that whenever  $c_2 > \frac{1}{c_1^2}$ ,  $m(n, n/c_1, nc_2)$  grows exponentially. How does  $m(n, n/c_1, nc_2)$  grow whenever  $c_2 \in \left[\frac{2}{c_1^3 + c_1^2}, \frac{1}{c_1^2}\right]$ ?

We have shown that  $\pi\pi(n)$  never exceeds  $\pi(n) - \pi(\frac{n}{2}) + \pi(\sqrt{n})$ . We hypothesize that  $\pi\pi(n) = \pi(n) - \pi(\frac{n}{2}) + \pi(\sqrt{n})$  for all  $n \geq 55$ . A simple method to select a maximally-sized set of relatively prime integers is to take the square of each prime between  $\sqrt{\frac{n}{2}}$  and  $\sqrt{n}$ ,

---

<sup>3</sup>Suppose that  $\ell \geq \gamma + 1$  and we have an  $(n, \ell + 1, \gamma)$ -sharing set family  $S_1, \dots, S_m \subseteq [n]$  of size  $m$ . We can form a  $(n, \ell, \gamma)$ -sharing set family  $S'_1, \dots, S'_m \subseteq [n]$  by picking some element  $s_i \in S_i$  setting  $S'_i = S_i - \{s_i\}$  for each  $i \in [m]$ . Observe that this argument does not apply whenever  $\ell = \gamma$  because then we might have  $S'_i = S'_j$  for  $i \neq j$ .

and the product of the  $j$ 'th prime less than  $\sqrt{\frac{n}{2}}$  and the  $k$ 'th prime greater than  $\sqrt{n}$ , for  $j$  from 1 to  $\pi(\sqrt{n})$  and  $k = j$  unless this would make the product less than  $\frac{n}{2}$  in which case  $k$  is chosen to be the minimum value greater than the previous  $k$  so that the product is greater than  $\frac{n}{2}$ . With the aid of a computer we have shown this equation true for all  $n$  from 1 to 100,000, except for 51, 52, 53, and 54.

## References

- [BBD13] Jeremiah Blocki, Manuel Blum, and Anupam Datta. Naturally rehearsing passwords. In Kazuo Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013*, volume 8270 of *Lecture Notes in Computer Science*, pages 361–380. Springer Berlin Heidelberg, 2013.
- [Che52] Herman Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, 23(4):493–507, 1952.
- [EFF85] Paul Erdős, Peter Frankl, and Zoltán Füredi. Families of finite sets in which no set is covered by the union of others. *Israel Journal of Mathematics*, 51(1-2):79–89, 1985.
- [EH63] P Erdős and H Hanani. On a limit theorem in combinatorial analysis. *Publ. Math. Debrecen*, 10:10–13, 1963.
- [ER56] P Erdős and A Renyi. On some combinatorial problems. *Publ. Math. Debrecen*, 4:398–405, 1956.
- [Eul82] Leonhard Euler. *Recherches sur une nouvelle espece de quarres magiques*. Zeeuwsch Genootschap, 1782.
- [NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.
- [Ram19] Srinivasa Ramanujan. A proof of bertrand's postulate. *Journal of the Indian Mathematical Society*, 11:181–182, 1919.
- [Röd85] Vojtěch Rödl. On a packing and covering problem. *European Journal of Combinatorics*, 6(1):69–78, 1985.
- [RRV99] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in trevisan's extractors. In *Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing*, STOC '99, pages 149–158, New York, NY, USA, 1999. ACM.
- [Son09] Jonathan Sondow. Ramanujan primes and bertrand's postulate. *American Mathematical Monthly*, 116(7):630–635, 2009.
- [Tre01] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

## 7 Missing Proofs

**Reminder of Theorem 7.**  $\forall 0 < c_2 < 1, n, c_1 \in \mathbb{N}$  such that  $c_1 | n$ .  $m(n, \frac{n}{c_1}, c_2 n) = c_1$  iff  $c_2 < \frac{2}{c_1^3 + c_1^2}$ .

*Proof of theorem 7.* Suppose that for some valid  $n, c_1, c_2$  there is an  $(n, \ell, \gamma)$ -sharing set family of size  $c_1 + 1$ . By equation 1, the number of elements used by such a set family must be at least:

$$(c_1 + 1)\ell - \frac{c_1(c_1 + 1)\gamma}{2} \leq n \quad (2)$$

Taking advantage of the fact that  $\ell = \frac{n}{c_1}$  and  $\gamma = c_2 n$ , the inequality can be simplified:

$$\begin{aligned} n + \ell - \frac{c_1(c_1 + 1)\gamma}{2} &\leq n \\ \ell &\leq \frac{c_1(c_1 + 1)\gamma}{2} \\ \frac{n}{c_1} &\leq \frac{c_1(c_1 + 1)c_2 n}{2} \\ 2n &\leq (c_1^3 + c_1^2)c_2 n \\ \frac{2}{c_1^3 + c_1^2} &\leq c_2 . \end{aligned}$$

Thus, all set families of size  $c_1 + 1$  or greater must have  $c_2 \geq \frac{2}{c_1^3 + c_1^2}$ , and  $c_2 < \frac{2}{c_1^3 + c_1^2}$  guarantees the set family will have a size of at most  $c_1$ .

Since  $c_1 \ell = n$ , it is possible to make a family of size  $c_1$  for any value of  $c_2$  by simply choosing sets that share no elements. Therefore, the size of the largest possible set family for any  $n, \ell, \gamma$  meeting the specified conditions is  $c_1$  if  $c_2 < \frac{2}{c_1^3 + c_1^2}$ .

If  $c_2 \geq \frac{2}{c_1^3 + c_1^2}$ , there will always exist a set family of size  $\geq c_1 + 1$ . To create such a family, choose  $c_1 + 1$  sets such that each of them shares  $\gamma$  elements with each of the others. This will be possible as long as:

$$\begin{aligned} c_1 \gamma &\leq \ell \\ n c_1 c_2 &\leq \frac{n}{c_1} \\ c_1^2 c_2 &\leq 1 \\ \frac{2c_1^2}{c_1^3 + c_1^2} &\leq 1 . \end{aligned}$$

Since this final inequality is true for all possible values of  $c_1$ , it will such a set family can always be created, and its size will be, as shown earlier,  $n$  when  $c_2 = \frac{2}{c_1^3 + c_1^2}$ . Since increasing  $c_2$  will not eliminate any possible set families, no  $n, \ell, \gamma$  satisfying the conditions with  $c_2 \geq \frac{2}{c_1^3 + c_1^2}$  will have a maximum family size  $< c_1 + 1$ . Therefore, the size of the largest possible set family for a valid  $n, \ell, \gamma$  will be  $c_1$  iff  $c_2 < \frac{2}{c_1^3 + c_1^2}$ .  $\square$

The proof of theorem 9 is based on standard concentration bounds due to Chernoff. We use the specific form from Theorem 10. We demonstrate the existence of an  $(n, \ell, \gamma)$ -sharing

set family of exponential size by showing that the probability of obtaining such a set family through random selection is non-zero.

**Theorem 10.** [Che52] Let  $X_1, \dots, X_n \in [0, 1]$  be a sequence of independent random variables. Let  $S = \sum_{i=1}^n x_i$ , and let  $\mu = \mathbf{E}[S]$ . Then for all  $\delta \geq 0$

$$\Pr[S \geq \mu + \delta n] \leq e^{-2n\delta^2}.$$

**Reminder of Theorem 9.**  $\forall c_2 > 0, n, c_1 \in \mathbb{N}$  such that  $c_1 | n$ .  $m(n, \frac{n}{c_1}, c_2 n) > \exp(O(n))$  if  $c_2 > \frac{1}{c_1^2} + \epsilon$ .

*Proof of Theorem 9.* We create an  $(n, \ell, \gamma)$ -sharing set family by creating sets in the following manner: Independently choose random integers  $r_i^j$  each in the range  $0 \leq r_i < c_1$  for  $j \in [m]$  and  $i \in \{0, \dots, \ell - 1\}$ . Let  $S_j = \bigcup_{i=0}^{\ell-1} \{ic_1 + r_i^j\}$ . Given two such sets,  $S_j, S_k$  let

$$x_i = \begin{cases} 1 & : r_i^j = r_i^k \\ 0 & : r_i^j \neq r_i^k \end{cases}$$

Then the number of elements shared by  $S_j$  and  $S_k$  is

$$S_j \cap S_k = \sum_{i=0}^{\ell-1} x_i.$$

Let  $\mu = \mathbf{E}[S_j \cap S_k] = \frac{n}{c_1^2}$  denote the expected number of shared elements. The probability that two such sets share more than  $\gamma$  elements, given  $c_2 = \frac{1}{c_1^2} + \epsilon$  is

$$\begin{aligned} \Pr[|S_j \cap S_k| > \gamma] &= \Pr\left[\sum_{i=0}^{\ell-1} x_i > c_2 n\right] \\ &= \Pr\left[\sum x_i > \frac{n}{c_1^2} + n\epsilon\right] \\ &\leq \Pr\left[\sum x_i \geq \mu + \epsilon n\right] \\ &\leq e^{-2n\epsilon^2} \end{aligned}$$

with the last step by Theorem 10. Thus the probability that two randomly selected sets share more than  $\gamma$  elements is at most  $e^{-2n\epsilon^2}$ .

An  $(n, \ell, \gamma)$ -sharing set family of size  $m$  will contain  $\binom{m}{2}$  pairs of sets. The probability that the family is valid, with none of the sets sharing more than  $\gamma$  elements is

$$\begin{aligned} \Pr[\exists j \neq k : |S_j \cap S_k| > \gamma] &\leq \binom{m}{2} \Pr[|S_j \cap S_k| > \gamma] \\ &\leq \binom{m}{2} e^{-2n\epsilon^2} \\ &\leq m^2 e^{-2n\epsilon^2} \end{aligned}$$

by the union bound. For  $m < e^{n\epsilon^2}$ , this probability will be less than 1, meaning there is a non-zero chance of forming a valid set family of size  $m$  by random selection and therefore such a family must exist.  $\square$